

Michael University

Introduction to Cybersecurity

DRAFT

Spring Semester 2027

Online Course

Course Designer:

Dr. Richard W. Clark

Dean, International Studies

Michael University

mccuniversity@gmail.com

Introduction to Cybersecurity (3 credits)

Undergraduate Course Syllabus

Course Title: Introduction to Cybersecurity
Credit Hours: 3
Program Fee: $5,800.00
Course Format: Fully Online – Asynchronous
Course Length: 8 Weeks (Modules)
Academic Level: Undergraduate
Prerequisites: None
Department: Computer Science
Michael University
Instructor: Dr. Richard W. Clark
Email: mccuniversity@gmail.com
Office Hours: By virtual appointment
Learning Management System: Zoom / Google Tools

I. COURSE DESCRIPTION

Introduction to Cybersecurity provides students with a foundational understanding of cybersecurity concepts, technologies, practices, and emerging challenges in an increasingly interconnected digital environment.

Students explore the principles of information security, cybersecurity threats, network protection, encryption, identity and access management, data privacy, risk management, incident response, and emerging cybersecurity technologies.

The course emphasizes the application of cybersecurity principles to personal, educational, business, government, and organizational environments. Through case studies, online discussions, interactive exercises, and applied learning experiences, students develop the ability to recognize cybersecurity threats, evaluate vulnerabilities, assess risks, and recommend appropriate protective strategies.

This course is designed for undergraduate students from diverse academic disciplines. No previous programming, computer networking, or cybersecurity experience is required.

II. COURSE PURPOSE AND RATIONALE

Cybersecurity has become an essential component of personal, professional, organizational, and national security. Individuals and organizations increasingly depend

DRAFT

on digital technologies to communicate, conduct business, store information, and manage critical operations.

This course introduces students to the knowledge and skills necessary to understand and respond responsibly to cybersecurity challenges.

The course is interdisciplinary and appropriate for students majoring in information technology, business, criminal justice, education, healthcare, communications, public administration, and related fields.

III. COURSE LEARNING OUTCOMES

Upon successful completion of this course, students will be able to:

1. Explain fundamental cybersecurity principles, concepts, terminology, and the importance of information security.

2. Identify and distinguish common cybersecurity threats, vulnerabilities, and attack methods.

3. Describe fundamental network security practices and technologies used to protect digital environments.

4. Explain the role of encryption, authentication, authorization, and access management in protecting information.

5. Evaluate cybersecurity issues involving data privacy, ethics, legal responsibilities, and organizational accountability.

6. Conduct a basic cybersecurity risk assessment and recommend appropriate risk mitigation strategies.

7. Analyze cybersecurity incidents and explain appropriate incident response and recovery procedures.

8. Develop a basic cybersecurity protection plan for a selected organization.

IV. INSTRUCTIONAL APPROACH

The course uses an asynchronous online instructional model emphasizing active learning, student engagement, critical thinking, and practical application.

Instructional methods include:

- Instructor-developed video lectures and presentations.
- Assigned readings and online instructional resources.

DRAFT

- Interactive tutorials and demonstrations.
- Weekly online discussion forums.
- Cybersecurity case studies.
- Guided cybersecurity exercises and simulations.
- Module knowledge checks.
- An applied final cybersecurity protection capstone project.

Students should plan to spend approximately 9–12 hours per week on course-related activities, including instruction, readings, discussions, assignments, and independent study. Actual time will vary according to individual experience and assignment complexity.

V. REQUIRED AND RECOMMENDED INSTRUCTIONAL RESOURCES

Required technology:

- Reliable internet access.
- Desktop or laptop computer.
- Current web browser.
- Word processing and presentation software.
- Ability to view instructional videos and participate in online discussions.

Textbook(s):

Foundations of Cybersecurity: A Straightforward Introduction, 2nd Edition, Andress, J. (2026). ISBN: 9781718504400. No Starch Press
Available on Amazon: https://www.amazon.com/clp/1718504403?lv=shuf&channelId=500
Also available on Kindle.

Recommended resources:

1. National Institute of Standards and Technology (NIST), Cybersecurity Framework 2.0. https://www.nist.gov/
2. Cybersecurity and Infrastructure Security Agency (CISA), cybersecurity awareness resources. https://www.cisa.gov/

DRAFT

3. National Cybersecurity Alliance, online safety resources. https://www.cybersecurityintelligence.com/national-cybersecurity-alliance-9303.html
4. Cisco Networking Academy, introductory cybersecurity educational materials. https://www.cisco.com/site/us/en/learn/training-certifications/training/netacad/index.html#tabs-35d568e0ff-item-4bd7dc8124-tab
5. Current introductory cybersecurity textbook or approved open educational resources.

The instructor will provide specific readings, videos, and supplemental resources through Google Slides, PowerPoint, Zoom and other tools.

VI. COURSE ORGANIZATION AND WEEKLY SCHEDULE

The course consists of eight instructional modules. Each module includes measurable learning objectives, instructional materials, an applied learning activity, an online discussion, and an assessment.

MODULE 1 – INTRODUCTION TO CYBERSECURITY

MODULE 2 – CYBERSECURITY THREATS AND VULNERABILITIES

MODULE 3 – NETWORK AND SYSTEMS SECURITY

MODULE 4 – DATA PROTECTION, ENCRYPTION, AND ACCESS MANAGEMENT

MODULE 5 – CYBERSECURITY, PRIVACY, ETHICS, AND LEGAL ISSUES

MODULE 6 – RISK MANAGEMENT AND ORGANIZATIONAL CYBERSECURITY

MODULE 7 – CYBERSECURITY INCIDENT RESPONSE AND RECOVERY

MODULE 8 – EMERGING CYBERSECURITY CHALLENGES AND FINAL APPLICATION

FINAL PROJECT: Organizational Cybersecurity Protection Plan

Students will develop a comprehensive introductory cybersecurity protection plan for a selected organization.

VII. COURSE GRADING AND ASSESSMENT

The final course grade will be calculated using the following weighted categories:

Assessment Category	Weight
Eight Module – Realistic-Based Scenarios (5% each)	40%

DRAFT

Eight Online Discussions	15%
Four Applied Cybersecurity Exercises	20%
Final Cybersecurity Protection Plan	25%
TOTAL	**100%**

Grade Scale

Letter Grade	**Percentage**
A	90–100%
B	80–89%
C	70–79%
D	60–69%
F	Below 60%

Individual assessment grades will be calculated using the stated category weights as per university guidelines and instructor criteria.

VIII. ASSIGNMENT AND ASSESSMENT RUBRICS

The following rubrics establish consistent performance expectations and provide transparent evaluation criteria.

RUBRIC 1: ONLINE DISCUSSION PARTICIPATION

Weight: 15% of final course grade.

Each of the eight discussions is evaluated using the following rubric. The category score is calculated as the average of the eight discussion scores.

Criterion	**Exemplary (4)**	**Proficient (3)**	**Developing (2)**	**Beginning (1)**
Content knowledge (30%)	Demonstrates comprehensive understanding of the topic	Demonstrates accurate understanding	Demonstrates partial understanding	Demonstrates limited understanding
Critical thinking (30%)	Provides insightful analysis and relevant examples	Provides meaningful analysis	Provides limited analysis	Provides little or no analysis

DRAFT

Engagement and responses (25%)	Initial post and at least two substantive peer responses	Initial post and two relevant responses	Incomplete or limited peer interaction	Minimal or no peer interaction
Writing and professionalism (15%)	Clear, organized, professional, and well-supported	Generally clear and organized	Some organizational or writing issues	Difficult to follow or unprofessional

Performance standards:

- Exemplary: 90–100%
- Proficient: 80–89%
- Developing: 70–79%
- Beginning: Below 70%

RUBRIC 2: APPLIED CYBERSECURITY EXERCISES

Weight: 20% of final course grade.

Each of the four applied exercises will be graded using this rubric.

Criterion	**Exemplary (4)**	**Proficient (3)**	**Developing (2)**	**Beginning (1)**
Identification of security issues (30%)	Identifies all major relevant threats and vulnerabilities	Identifies most major issues	Identifies some relevant issues	Identifies few relevant issues
Application of concepts (30%)	Applies cybersecurity principles accurately and effectively	Applies concepts appropriately	Demonstrates partial application	Demonstrates limited application
Recommendations (25%)	Provides practical, well-justified recommendations	Provides appropriate recommendations	Recommendations lack sufficient detail	Recommendations are inappropriate or missing
Organization and communication	Clear, organized, and	Generally organized and	Some clarity or organization	Disorganized or difficult to

DRAFT

(15%)	professionally presented	understandable	problems	understand

RUBRIC 3: Realistic-Based Scenarios

Weight: 40% of final course grade.

Each of the eight modules will include Realistic-based Scenarios worth 40% of the final course grade.

Weekly Scenario-Based Assessments

Assessment Overview

Week	Topic	Assessment	Points
1	Cybersecurity Fundamentals	Identifying Assets, Threats, and Vulnerabilities	25
2	Cyber Threats	Phishing Incident Analysis	25
3	Network Security	Securing a Small Business Network	25
4	Authentication & Access	Access Control Review	25
5	Data Security & Privacy	Protecting Sensitive Information	25
6	Risk & Incident Response	Ransomware Response Scenario	25
7	Ethics & Professional Responsibility	The Ethical Security Dilemma	25
8	Emerging Trends	Cybersecurity in the Future	25
Total			200

RUBRIC 4: FINAL CYBERSECURITY PROTECTION PLAN

Weight: 25% of final course grade.

The final project is the culminating assessment of student learning and application of course concepts.

Criterion	Weight	Exemplary Performance
Organizational overview	10%	Provides a clear and relevant organizational

DRAFT

		description
Threat and vulnerability identification	20%	Identifies and evaluates at least five relevant cybersecurity risks
Security policies and recommendations	20%	Develops practical, appropriate security recommendations
Data and network protection	15%	Integrates appropriate data protection, authentication, and network security measures
Incident response and recovery	15%	Provides a logical and effective incident response and recovery strategy
Implementation priorities	10%	Establishes realistic implementation priorities and responsibilities
Professional presentation and organization	10%	Demonstrates clear writing, organization, and appropriate documentation
TOTAL	**100%**	

Final project performance standards:

- Exemplary: 90–100%
- Proficient: 80–89%
- Developing: 70–79%
- Beginning: Below 70%

IX. COURSE POLICIES AND STUDENT EXPECTATIONS

Attendance and Participation

Because this course is asynchronous, attendance is measured through meaningful academic participation, for example online discussions, presentations, etc.

Students are expected to:

- Access the course regularly.
- Review weekly instructional materials.
- Participate in assigned discussions.
- Complete assignments and assessments.
- Communicate with the instructor when academic difficulties arise.

DRAFT

Students should follow the university's official attendance and participation policies.

Late Work Policy

Assignments should be submitted by the deadlines established by the instructor.

Unless otherwise approved:

- Late submissions within seven calendar days may receive a deduction of 10% of the assignment's earned score.
- Submissions more than seven days late may not be accepted.
- Exceptions may be granted for documented emergencies or circumstances consistent with university policy.

Institutional policies take precedence over this syllabus provision.

Academic Integrity

Students are expected to demonstrate honesty, originality, and ethical conduct in all academic activities.

Academic misconduct includes:

- Plagiarism.
- Unauthorized collaboration.
- Fabrication of information or sources.
- Cheating on quizzes and examinations.
- Unauthorized use of another student's work.
- Unauthorized use of artificial intelligence tools.

Students must follow the university's academic integrity policy.

Artificial Intelligence Use

Artificial intelligence tools may be used for approved learning activities when permitted by the instructor.

Students must:

- Disclose AI assistance when required.
- Verify the accuracy of AI-generated information.
- Cite sources appropriately.

DRAFT

- Avoid submitting AI-generated work as original work when prohibited.
- Never enter confidential personal or organizational information into public AI systems.

AI tools may not be used to bypass learning objectives or compromise academic integrity.

Online Communication and Netiquette

Students are expected to communicate respectfully and professionally.

Online discussions should demonstrate:

- Respect for differing perspectives.
- Constructive feedback.
- Professional language.
- Relevant and evidence-based contributions.
- Appropriate citation of outside sources.

Accessibility and Accommodations

The university is committed to providing accessible learning opportunities.

Students requiring accommodations should contact the university's designated accessibility services office. Course materials and activities will be designed to support accessibility and comply with applicable institutional requirements.

Technology and Technical Support

Students are responsible for maintaining access to appropriate technology and submitting assignments online as per instructor.

Technical difficulties should be reported promptly to university technical support and the instructor.

X. INSTRUCTOR RESPONSIBILITIES

The instructor will:

1. Provide weekly instructional materials and announcements.
2. Facilitate online discussions and encourage student engagement.
3. Provide timely feedback on assignments.
4. Clarify course expectations and assessment requirements.

DRAFT

5. Maintain regular communication with students.
6. Provide guidance on cybersecurity learning resources.
7. Monitor student progress and identify opportunities for additional support.

The instructor will normally respond to student inquiries within two business days and provide assignment feedback within seven calendar days, subject to university policy and course scheduling.

XI. COURSE ALIGNMENT AND ASSESSMENT MATRIX

The following matrix demonstrates the relationship between course learning outcomes, instructional modules, and assessments.

Course Learning Outcome	Module(s)	Primary Assessment
1: Explain cybersecurity principles	1	Real-based scenarios and discussion
2: Identify threats and vulnerabilities	2	Real-based scenarios and threat analysis
3: Describe network security practices	3	Real-based scenarios and network assessment
4: Explain encryption and access management	4	Real-based scenarios and access plan
5: Evaluate ethical, legal, and privacy issues	5	Case study and discussion
6: Conduct a basic risk assessment	6	Risk assessment exercise
7: Analyze incidents and recovery procedures	7	Incident response exercise
8: Develop a cybersecurity protection plan	8	Final project

XII. COURSE EVALUATION AND CONTINUOUS IMPROVEMENT

The effectiveness of the course will be evaluated through:

- Student achievement of course learning outcomes.
- Performance on Real-based scenarios and applied assignments.
- Quality of final cybersecurity protection plans.
- Student course evaluations.

DRAFT

- Student engagement and course completion rates.
- Instructor reflection and review of course materials.

Note: Course content and instructional resources will be reviewed annually to reflect changes in cybersecurity technologies, emerging threats, industry practices, and applicable regulatory requirements.

XIII. CONCLUDING COURSE STATEMENT

Introduction to Cybersecurity provides undergraduate students with the foundational knowledge, analytical skills, and practical strategies necessary to recognize cybersecurity threats and respond responsibly to security challenges in personal and organizational environments.

Through an integrated online learning experience emphasizing theoretical understanding, practical application, ethical decision-making, and critical thinking, students will develop cybersecurity competencies that are relevant across academic disciplines and professional careers.

END OF SYLLABUS

DRAFT